WHAT IS CLAIMED IS:

1. A cryptographic communication method for communicating information through a ciphertext between entities, comprising the steps of:

generating a secret key of each entity by using mapping at a point on an algebraic curve based on identity information of each entity and secret information;

generating at a first entity a first common key by using the secret key of the first entity and a public key obtained by mapping at a point on the algebraic curve based on identity information of a second entity;

encrypting at the first entity a plaintext into a ciphertext by using the generated first common key and transmitting the ciphertext to the second entity;

generating at the second entity the same second common key as the first common key by using the secret key of the second entity and a public key obtained by mapping at a point on the algebraic curve based on identity information of the first entity; and

decrypting at the second entity the transmitted ciphertext into a plaintext by using the generated second common key.

2. A method for generating a common key between a first entity and a second entity, comprising the steps of:

generating a secret key of the first entity by using mapping at a point on an algebraic curve based on identity information of the first entity and secret information;

generating a public key of the second entity by using mapping at a point on the algebraic curve based on identity information of the second entity; and

generating a common key between both entities by using the secret key and public key thus generated.

3. The common key generating method according to claim 2, wherein the common key is generated by using pairing defined on the algebraic curve.

4. A method for sharing a key without a preliminary communication between entities, comprising the steps of:

obtaining a secret key of a first entity;

obtaining a public key of a second entity, the public key being obtained by mapping at a point on an algebraic curve based on identity information of the second entity; and

generating a common key between the first entity and the second entity by using the secret key and the public key.

5. The key sharing method according to claim 4, wherein the algebraic curve is an algebraic curve in which a discrete logarithm problem defined thereon cannot be solved in a polynomial time.

6. The key sharing method according to claim 4, wherein numeric values which are inverse to each other are generated in a process of an operation in respective entities when sharing the key between the first entity and the second entity.

7. The key sharing method according to claim 4, wherein a plurality of public keys are generated based on the identity information of each entity.

8. A method for sharing a key without a preliminary communication between both entities based on respective identity information of the entities, wherein pairing defined on an algebraic curve is used.

9. The key sharing method according to claim 8, wherein the pairing is Weil pairing or Tate pairing.

10. A method for sharing a key without a preliminary communication between a first entity and a second entity based on respective identity information of the entities, wherein pairing defined on an algebraic curve is used to share a key by utilizing a secret key generated by using mapping at a point on the algebraic curve based on the identity information of the first entity and secret information and a public key obtained by mapping at a point on the algebraic curve based on the identity information of the second entity.

11. A method for generating a common key based on the key sharing method according to claim 6, wherein the common key is generated by utilizing a relationship of inverse between the numeric values.

12. A method for generating a secret key of an entity based on identity information of the entity, wherein the secret key is generated by using mapping at a point on an algebraic curve based on the identity information of the entity and secret information.

13. A method for generating a secret key of an entity based on identity information of the entity, wherein the secret key is generated by using mapping at a point on an algebraic curve based on a value obtained by causing a one-way function to act on the identity information of the entity and secret information.

14. A secret key generating device for generating a secret key of an entity based on identity information of the entity, comprising:

a controller capable of performing the following operations;

(i) obtaining a mapping value by mapping at a point on an algebraic curve based on the identity information of the entity; and

(ii) generating the secret key by using the mapping value and secret information.

15. A common key generating device for generating a common key from a secret key based on identity information of a first entity and a public key based on identity information of a second entity to be a communication partner, comprising:

a controller capable of performing the following operations;

(i) obtaining a mapping value as the public key by mapping at a point on an algebraic curve based on the identity information of the second entity; and

(ii) generating a common key by using the mapping value and the secret key.

16. A cryptographic communication system for permitting a plurality of entities to mutually perform an encrypting process for encrypting into a ciphertext information of a plaintext to be transmitted and a decrypting process for decrypting the transmitted ciphertext into a plaintext, comprising:

a center generating a secret key of each entity by using mapping at a point on an algebraic curve based on identity information of each entity and self-secret information and sending the secret key to each entity; and

a plurality of entities generating a common key to be used for the encrypting process and the decrypting process by using the self-secret key sent from said center and a public key obtained by mapping at a point on an algebraic curve based on identity information of an entity to be communicated.

17. A computer memory product having computer readable program code means for causing a computer to generate a secret key of an entity, said computer readable program code means comprising:

program code means for causing the computer to obtain a mapping value as a public key by mapping at a point on an algebraic curve based on identity information of the entity; and

program code means for causing the computer to generate the secret key by using the mapping value and secret information.

18. A computer memory product having computer readable program code means for causing a computer to generate, on a first entity side, a common key to be used for an encrypting process from a plaintext to a ciphertext and a decrypting process from the ciphertext to the plaintext, in an cryptographic communication system said computer readable program code means comprising:

program code means for causing the computer to input a secret key of the first entity;

program code means for causing the computer to obtain a mapping value as a public key by mapping at a point on an algebraic curve based on identity information of a second entity to be a communication partner; and

program code means for causing the computer to generate the common key by using the mapping value and the input secret key.

19. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a secret key of an entity, comprising:

a code segment for causing the computer to obtain a mapping value as a public key by mapping at a point on an algebraic curve based on identity information of the entity; and

a code segment for causing the computer to generate the secret key by using the mapping value and secret information.

20. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate, on a first entity side, a common key to be used for an encrypting process from a plaintext to a ciphertext and a decrypting process from the ciphertext to the plaintext in an cryptographic communication system, comprising:

a code segment for causing the computer to input a secret key of the first entity;

a code segment for causing the computer to obtain a mapping value as a public key by mapping at a point on an algebraic curve based on identity information of a second entity to be a communication partner; and

a code segment for causing the computer to generate the common key by using the mapping value and the input secret key.